المدن
جريدة إلكترونية مستقلة .. وفي رواية أخرى

الرئيسية محطات

احتكار غوغل لأندرويد: الهواتف منصة للتنصت والترصد والاحتيال

نافع سعد | الأحد 2025/07/06



ثغرات أمنية خطيرة في نظام أندرويد تتيح لبرمجيات خبيثة استغلال ضعف نماذج الأذونات (Getty)

مشاركة عبر

حجم الخط

نظام أندرويد، الذي انطلق كنظام تشغيل مفتوح المصدر، تحوّل تدريجياً إلى أحد أكثر البيئات المقفلة في عالم البرمجيات. فعند انطلاق "مشروع أندرويد مفتوح المصدر" (AOSP)، كان بإمكان أي شخص الاطّلاع على كل سطر من الكود الأساسي وتعديله وإعادة توزيعه بموجب تراخيص Apache 2.0وGPL v2. وقد غذّى هذا البناء الشفاف للابتكار مجتمعاً عالمياً من المطورين الذين شرعوا في استكشاف واجهات مستخدم ثورية وبناء التطبيقات من دون قيود. لكن الأجهزة التي نحملها اليوم تخضع لشبكة معقّدة من القيود التعاقدية والتشغيلية، وبرامج غير مرئية تثقل جهازك بجاذبية غوغل.

آليات السيطرة

عندما استحوذت غوغل على شركة أندرويد عام 2005 مقابل نحو خمسين مليون دولار، لم يكن هدفها مجرد رعاية مشروع مفتوح المصدر. ففي عام 2007، أطلقت الشركة "اتحاد الأجهزة المحمولة المفتوحة" (Open Handset Alliance)، الذي ضمّ عشرات الشركات من صانعي الأجهزة ومشغّلي شبكات الاتصالات ومصنّعي شرائح المعالجات، سعياً لتوحيد معايير نظام أندرويد. ورغم المظهر الإيجابي لتعزيز التوافق حول بيئة التشغيل، فقد تحوّل الأمر في الواقع إلى نموذج احتكاري. إذ يُلزم هذا الاتفاق الشركات المصنّعة بتضمين حزمة خدمات غوغل (Google Mobile Services) التي تشمل تطبيقات أساسية مثل Gmail ومحرّك بحث غوغل ومتجر Play وخرائط غوغل، إضافة إلى واجهات برمجة التطبيقات (APIs) الضرورية لتشغيل التطبيقات وخدماتها. ومن يرفض هذه الشروط يفقد حق استخدام العلامات التجارية لغوغل والحصول على التحديثات الأمنية الحيوية. وهكذا تحوّل مشروع كان يُفترض أن يكون مفتوحاً إلى منظومة مقفلة تحكمها غوغل.

من متجر Play، مُدمجة ضمن صورة النظام ومخزنة في المجلد "/system/priv-app"، وتحمل توقيعاً رقمياً بمفتاح غوغل الخاص. يمنح هذا التوقيع لهذه التطبيقات صلاحيات استثنائية؛ إذ تحصل تلقائياً على أذونات نظامية واسعة أثناء التثبيت، كالوصول إلى جهات الاتصال والميكروفون والكاميرا والموقع، دون إشعار المستخدم. علاوةً على ذلك، تستطيع هذه التطبيقات تفعيل واجهات برمجة داخلية مخفية غير متاحة للمطورين الخارجيين. بفضل هذه الإمكانيات، يمكن لتطبيقات غوغل مراقبة الأصوات المحيطة وقراءة الرسائل النصية وسجلات المكالمات وتتبع الموقع بدقّة. والنتيجة هي رصد شامل للسلوكيات والبيئة الرقمية للمستخدم دون إدراكه.
تمثّل خدمات غوغل بلاي وسيطاً خفياً يربط التطبيقات ببنية غوغل المغلقة، حيث تُقدّم وظائف حيوية مثل الإشعارات الفورية ومعالجة مدفوعات التطبيقات وتأكيد هوية المستخدم وتتبع الموقع الدقيق وفحص أمان الجهاز. لكن هذه الكفاءة لا تأتي من دون ثمن، فهي تتمتّع بصلاحيات نظامية تسمح لها بتجاوز آليات الأذونات العادية، وتعمل في الخلفية دون سؤال المستخدم أو إشعاره.

الثغرات الأمنية: تهديدات متعددة المستويات

رغم القوة التقنية التي تتمتّع بها غوغل، تبرز ثغرات أمنية خطيرة في نظام أندرويد تتيح لبرمجيات خبيثة استغلال ضعف نماذج الأذونات ومسارات التثبيت. فبرمجيات تجسّس متطوّرة مثل "بيغاسوس" (التي طوّرتها مجموعة NSO الإسرائيلية) تخترق الأجهزة عبر ثغرات "نقرة صفرية" في تطبيقات المراسلة من دون تفاعل من المستخدم، لتحصل على صلاحيات جذرية (root privilege) وتنفّذ تنصّتاً شاملًا على المكالمات والرسائل والموقع والكاميرا من دون أي أثر. وقد سجّلت مختبرات Citizen Lab اختراقات "بيغاسوس" في خمسٍ وأربعين دولة، مستهدفةً صحافيين ونشطاء سياسيين وأفراد عائلاتهم.
وبجانب برامج التجسّس الحكومية، تنتشر تطبيقات احتيالية (مثل قارئات PDF)، تعمل بشكل خفي لسرقة الحسابات وكلمات المرور أو طلب أذونات لا علاقة لها بوظيفتها؛ كأن يطلب تطبيق ماسح رمز QR الإذن

خصوصيتك لجمع المعلومات بهدف تعزيز فعالية إعلاناتها أولاً وآخراً. غوغل، التي أنشأت بنية متقنة لجمع أكبر قدر ممكن من البيانات حولك باستخدام الميكروفون والموقع وكل ما على هاتفك، تحوّل هذا النظام نفسه إلى حصان طروادة لبرامج التجسّس والاحتيال.

استعادة السيطرة الرقمية

لمواجهة هذا المشهد المعقَّد المتمثل في المراقبة الخفيّة والتهديدات الرقمية، لا بدّ من الدفع باتجاه استراتيجية شاملة تستهدف المستخدمين والمطوّرين والجهات التنظيمية على حدّ سواء.

على مستوى المستخدمين: تكمن الخطوة الأولى في تعزيز اليقظة الدائمة عبر مراجعة أذونات التطبيقات بانتظام وسحب صلاحيات الوصول غير الضرورية، خصوصاً تلك المرتبطة بخدمات إمكانية الوصول وعرض النوافذ فوق التطبيقات الأخرى. كما يُفضّل استخدام جدران حماية مثلNetGuard لحظر الاتصالات المشبوهة لكل تطبيق. كذلك، يُستحسن إجراء بحث معمّق عن تطبيق VPNالذي تنوي استخدامه، إذ ليس جميع هذه التطبيقات آمنة.

على مستوى المطوّرين: فيستطيعون المساهمة في تحسين المشهد الأمني من خلال تقليل الاعتماد على خدمات غوغل المغلقة المصدر، واعتماد معايير مفتوحة مثل WebAuthnللمصادقة الآمنة، و Matrixأو WebPushللإشعارات، وبروتوكولات الهوية اللامركزية. ويُراعى تطبيق مبدأ "أقل الصلاحيات الممكنة" عند طلب الأذونات، مع توضيح أسباب كل طلب للمستخدمين، فضلًا عن إجراء مراجعات أمنية مستقلة لتعزيز الثقة في تطبيقاتهم.

على صعيد الجهات التنظيمية وشركات تصنيع الأجهزة: فيجب إلزام جميع التطبيقات المثبّتة مسبَقاً بطلب الأذونات بطريقة واضحة وسياقية عند التشغيل، وفرض الشفافية الكاملة حيال البرامج المضمّنة وتدفق البيانات وجداول التحديثات الأمنية. كما ينبغي تشجيع ودعم التفرعات والإصدارات المتعددة لأنظمة أندرويد عبر تبسيط الإجراءات التقنية وإرساء آليات اعتماد

إتاحة الكود المصدري. فهو يتطلب عقوداً شفافة، ونموذج أدوات متوازن، ورقابة مستمرة من جميع الأطراف المعنية. وفقط من خلال تفكيك مثلث السيطرة المتمثل في الاحتكار التعاقدي والوساطة المغلقة والمراقبة الخفيّة نستعيد السيادة على أجهزتنا التي لم تعد أدوات فحسب، بل امتداد لهويتنا الرقمية.

الأكثر قراءة



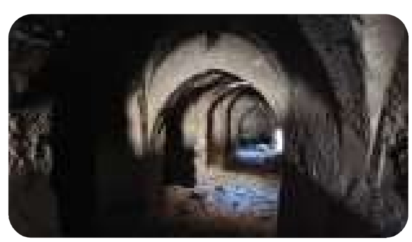
استجواب طلاب في الآداب 3: اللجنة منهمكة بتسريب المعلومات!



مفاضلة الجامعات في سوريا: تصحيح لمسار التعليم أم خيبة أمل؟



الذكاء الاصطناعي يحدث ثورة في طب العيون



بالفيديو: قلعة حارم التحفة الناجية من هولاكو تطلق نداء إنقاذ